REMARKS

Favorable reconsideration of this application, in view of the present amendments and in light of the following discussion, is respectfully requested.

Claims 15-28 are pending and amended. No new matter is introduced.

In the outstanding Office Action, Claims 15-28 were rejected under 35 U.S.C. § 102(e) as being anticipated by Talpade et al. (U.S. Patent Application Publication No. 2004/0148520, hereafter "Talpade").

In reply, Claim 15 is amended to recite, *inter alia*, a system for protecting a communication device against a denial-of-service attack, that includes:

> a monitoring device provided on a local area network including the communication device, the monitoring device being configured to monitor a packet transmitted to the communication device via an internet-service-provider network . . .
>
> wherein the monitoring device includes
>
> an attack detecting unit configured to detect an attack by the packet on the communication device, and
>
> a protection-request-information transmitting unit configured to transmit to the restricting device protection request information indicating a request for protection against the attack, the protection-request-information transmitting unit *updating the protection request information to exclude from restriction packets not included in the attack, based on a report transmitted from the restricting device* . . . (emphasis added).

Turning to the applied reference, Talpade describes a system for detecting and mitigating service attacks, which includes a sensor, an analysis engine and one or more filter routers.[1] Talpade describes that the sensor (234) monitors all traffic entering customer networks (204, 206) from the ISP network (202) through edge routers (226, 228).[2] Upon detection of an attack, the sensor (234) transmits an indication of the attack to the analysis

[1] Talpade at pages 1-2, paragraphs [0008] and [0009].
[2] Talpade at page 2, paragraph [0017]; see also Figure 2.

engine (232), which configures one or more filter routers (230) to advertise new routing information to each border router (220, 222, and 224) and each edge router (228).[3] The border routers(220, 222, 224) and the edge routers (228) redirect all packets, whether part of the attack or not, to the filter router (230) based on the new routing information, and the filter router (230) filters all attack traffic and forwards all non-attack traffic back to the ISP network (202) for delivery to the customer network (204, 206).[4] Talpade also describes that the sensor (234) may reside on existing hardware within the customer network and/or the ISP network.[5]

However, Talpade does not describe that the sensor (234) updates information regarding the attack based on reports received from the filter router (230). Instead, Talpade merely describes that the sensor (234) sends a service attack notification to the analysis engine (232) in order to receive protection. [6] Talpade also describes that the analysis engine (232) periodically updates the sensor filters (248) in the sensor (234) in order to keep the sensor current as service attack tools change and improve.[7] Nowhere, however, does Talpade describe that the filter router (230) transmits a report *to the sensor (234)*, much less that the sensor (234) updates its notification to the analysis engine (232) in order to exclude from restriction packets not part of the service attack based on any report provided by the filter router (230). Further, though Talpade describes that the analysis engine (232), not the sensor (234), may determine an entry point of a service attack by examining filter router (232) information, Talpade does not describe that either the analysis engine (232) or the sensor (234) determine whether individual packets are part of the attack based on this filter router (230) information. Conversely, amended Claim 15 recites that the monitoring device

---

[3] Id.
[4] Talpade at pages 2-3, paragraph [0017].
[5] Talpade at page 3, paragraph [0018].
[6] Talpade at page 2, paragraph [0017]; see also Figure 2.
[7] Talpade at page 3, paragraph [0020].

includes a protection-request-information transmitting unit that updates the protection request information to exclude from restriction packets not included in the attack, based on a report transmitted from the restricting device. Therefore, Talpade fails to disclose the claimed monitoring device, and amended Claim 15, together with its corresponding dependent claims, is believed to be in condition for allowance.

Moreover, amended Claim 21 recites features substantially similar to those recited in amended Claim 15 and is thus believed to be in condition for allowance, together with its corresponding dependent claims. Accordingly, it is respectfully requested that the rejection of Claims 15-28 under 35 U.S.C. § 102(e) be withdrawn.

For the reasons discussed above, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal allowance. Therefore, a Notice of Allowance for Claims 15-28 is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

James J. Kulbaski
Attorney of Record
Registration No. 34,648

Aldo Martinez
Registration No. 61,357

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)